80

Notice of Allowability	Application No.	Applicant(s)	
	10/775,485	VENKATESAN ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *05/24/2007 and interview held on 08/02/2007*.

2. ☒ The allowed claim(s) is/are *1-8 and 27-38*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8/14/07

DETAILED ACTION

1. Applicant's amendment filed on 13, 2007 has been entered. Claims 1-38 are pending.

Election/Restrictions

2. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-8, 27-38, drawn to a Matrix based hash function implementation, classified in class 380, subclass 37.

II. Claims 9-26, drawn to Encryption based on expander graphs, classified in class 380, subclass 28.

3. Restriction for examination purposes as indicated is proper because all these inventions listed in this action are independent or distinct for the reasons given above and there would be a serious search and examination burden if restriction were not required because one or more of the following reasons apply:

a. Inventions have acquired a separate status in the art in view of their different classification; and

b. The inventions require a different field of search (for example, searching different classes/subclasses or electronic resources, or employing different search queries);

4. During a telephone conversation with Bea Koempel-Thomas (Reg. No. 58213) on August 2, 2007 an election was made without traverse to prosecute the invention of

a Matrix based hash function implementation recited in claims 1-8, 27-38. Applicant representative authorized the examiner to cancel the non elected claims 9-26.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

6. Authorization for this examiner's amendment was given in a telephone interview with Bea Koempel-Thomas (Reg. No. 58213) on August 2, 2007.

7. The application has been amended as follows:

Claims 9-26 have been cancelled.

REASONS FOR ALLOWANCE

8. The following is an examiner's statement of reasons for allowance: **Menezes et al** discloses a general model for iterated hash functions. **Rosen** discloses Warshall's Algorithm, which is an efficient method for computing the transitive closure of a relation. **Aiello et al** discloses stretch functions used in combination with compression functions. However, claims 1, 27, 31 of the present application recite the following limitations "applying a block function to a first data input block from a plurality of data input blocks,

wherein the block function comprises a walk on a graph defined by a plurality of matrices, and repeatedly applying the block function to a next data input block from the plurality of data input blocks in accordance with a result of applying the block function to a previous data input block until the block function is applied to a final input block, and determining a hash value of the plurality of input blocks based on the result provided by the block function applied to the final input block, and providing the hash value of the plurality of input blocks to a computing environment." Each matrix in the above claims represents a vertex of the graph--the matrices describe the graph. None of the prior art of record recites the above-mentioned limitations. In light of the foregoing, the claims of the present application are found to be allowable over the prior art of record.

9. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is 571 270 1685. The examiner can normally be reached on Monday- Friday (every other friday off) EST.

11. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571 272 4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

12. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8/14/07